PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

STRÖM & GULLIKSSON IPC AB
P.O. Box 793
S-220 07 Lund
SUEDE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of mailing
(day/month/year) 30.03.2004

Applicant's or agent's file reference
W 5039-1008

IMPORTANT NOTIFICATION

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/EP 03/01474	14.02.2003	08.03.2002

Applicant
SONY ERICSSON MOBILE COMMUNICATIONS AB

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

The applicant's attention is drawn to Article 33(5), which provides that the criteria of novelty, inventive step and industrial applicability described in Article 33(2) to (4) merely serve the purposes of international preliminary examination and that "any Contracting State may apply additional or different criteria for the purposes of deciding whether, in that State, the claimed inventions is patentable or not" (see also Article 27(5)). Such additional criteria may relate, for example, to exemptions from patentability, requirements for enabling disclosure, clarity and support for the claims.

Name and mailing address of the international preliminary examining authority:

European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Authorized Officer

Kastlova, A

Tel. +49 89 2399-2348

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference W 5039-1008	**FOR FURTHER ACTION** See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP 03/01474	International filing date *(day/month/year)* 14.02.2003	Priority date *(day/month/year)* 08.03.2002
International Patent Classification (IPC) or both national classification and IPC H04Q7/38		
Applicant SONY ERICSSON MOBILE COMMUNICATIONS AB		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the opinion
   II ☐ Priority
   III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   IV ☐ Lack of unity of invention
   V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   VI ☐ Certain documents cited
   VII ☐ Certain defects in the international application
   VIII ☐ Certain observations on the international application

Date of submission of the demand 01.10.2003	Date of completion of this report 30.03.2004
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Fantacone, V Telephone No. +49 89 2399-7222 Europäisches Patentamt · European Patent Office · Office européen des brevets

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-15	as originally filed
15a	received on 20.02.2004 with letter of 20.02.2004

Claims, Numbers

1-45	received on 20.02.2004 with letter of 20.02.2004

Drawings, Sheets

1/5-5/5	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   □ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   □ the language of publication of the international application (under Rule 48.3(b)).

   □ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   □ contained in the international application in written form.

   □ filed together with the international application in computer readable form.

   □ furnished subsequently to this Authority in written form.

   □ furnished subsequently to this Authority in computer readable form.

   □ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   □ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   □ the description, pages:

   □ the claims, Nos.:

   □ the drawings, sheets:

5. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

see separate sheet

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-45
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-45
Industrial applicability (IA)	Yes:	Claims	1-45
	No:	Claims	

2. Citations and explanations

see separate sheet

Section I

1. The amendement made to dependent claims 10 and 11 extends the scope of the invention for which protection is sought beyond the content of the application as originally filed, contrary to Article 34 (2)(b) PCT. This relate in particular to the deleted feature "...in the **data string** of the message...", as this feature seems to be essential for carrying out the method claimed and said claims without said feature are not supported by an embodiment.

Section V

2. The following documents are referred to in this communication. Their numbering will be adhered to in the rest of the procedure:

   D1: XP 002 217 356
   D2: SyncML Device Management Security, Version 1.1, 2000-12-07

2.1 Document **D1** (see in particular the passages cited in the Search Report) discloses, according to all features of **claim 1**, a method for providing authentication (see page 20, line 1 to page 24, line 20) when messages are sent between an electronic communication apparatus (see "mobile phone" in page 7, lines 20-22) and a server (see "server" in page 7, lines 20-22) according to a synchronization protocol (SyncML), characterized in that:
an authentication method indicator (see XML Tag "type" on page 21, line 29-52; page 13, lines 37-40) is incorporated in an authentication protocol of the synchronization protocol (SyncML), wherein said authentication method indicator specifies an authentication method, which is determined based on an authentication capability of the apparatus (see inplicitly with "device capabilities" on section 2.7; "authentication information" on section 4.1, lines 3-4; "auth-basic" on section 4.1.1, line 11), according to which the authentication is executed (see page 20, line 1 to page 24, line 20).

The subject-matter of claim 1 therefore is **not new**, Articles 33(1) and (2) PCT.

2.2 The same consideration as made in above paragraph 1.1 regarding claim 1 are also valid for **independent claims 18 and 34** since they include the same feature combination as claim 1 in terms of apparatus claims which are directed to an electronic communication apparatus and, respectively, a server.

The subject-matter of independent claims 18 and 34 therefore is **not new**, Articles 33(1) and (2) PCT.

3. Remarks concerning formal defects in the international application:

In order to meet the requirements of Rule 5.1 (a) (ii) PCT, the most relevant prior art, i.e. the documents D1 and D2 should have been acknowledged by reference and briefly discussed in the introductory part of the description, preferably in such a way that the inventive merit of what is claimed can be readily understood.

Moreover, the Applicant's attention is drawn to the fact that, as a consequence of Rule 66.8(a) PCT the examiner is not permitted to carry out any amendments under the PCT procedure, however minor these may be.

Abbreviations

SyncML-DM	SyncML Device Management
SyncML-DS	SyncML Data Syncronization
SHA-1	Secure Hash Standard 1
Obex	Object Exchange protocol
http	Hyper Text Transfer Protocol
WSP	WAP Session Protocol

CLAIMS

1. A method for providing authentication when messages are sent between an electronic communication apparatus (1) and a server (3, 41, 51, 61) according to a synchronization protocol, **characterized in that** an authentication method indicator (AMI) is incorporated in an authentication protocol of the synchronization protocol, wherein said AMI specifies an authentication method, which is determined based on an authentication capability of the apparatus (1), according to which the authentication is to be executed.

2.The method according to claim 1, wherein the AMI is incorporated in a meta command of the synchronization protocol .

3. The method according to claim 1 or 2, wherein at least one authentication capability of the electronic communication apparatus is indicated in an authentication method list of an initialization message sent to the server (31, 41, 51, 61) for establishing a connection.

4. The method according to any of the previous claims, wherein any authentication data relating to the specified authentication method is incorporated in a data string of the synchronization protocol.

5. The method according to any of the previous claims, wherein the specified authentication method is GSM SIM authentication.

6. The method according to any of the claims 1-4, wherein the specified authentication method is UMTS USIM authentication, which also provides server authentication.

7. The method according to any of the claims 1-4, wherein the specified authentication method is WPKI or WIM authentication.

8. The method according to any of the claims 1-4, wherein the specified authentication method is SecureId or SafeWord authentication.

9. The method according to any of the claims 3-7, wherein the server (31, 41, 51, 61) determines the authentication capabilities of the electronic communication apparatus (1) based on the at least one authentication method listed in the authentication method list.

10. The method according to claim 9, wherein the server (31, 41, 51, 61) executes any necessary authentication steps according to one of the at least one authentication methods indicated in the authentication method list, and prepares and transmits a message to the electronic communication apparatus (1), comprising the AMI and any authentication data relating to the specified authentication method.

11. The method according to claim 10, wherein the electronic communication apparatus (1) receives the message, executes any necessary authentication steps according to the authentication method indicated by the AMI to generate an expected result, and prepares and transmits a response to the server, comprising the AMI, and any authentication data.

12. The method according to any of the claims 1-6 and 9-11, wherein integrity protection is provided by utilizing CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus (1) and the server (31,

41, 51, 61), respectively, when SIM/USIM authentication is executed, which CK/IK is used for generating MAC values and using a hashing function for computing a HMAC on a message to be sent.

13. The method according to any of the claims 7 or 9-11, wherein integrity protection is provided in that the server generates a integrity key, which is encrypted with the public key of the electronic communication apparatus (1), which is generated during the authentication procedure, said integrity key is sent to said apparatus (1), and utilized for generating MAC values and using a hashing function for computing a HMAC on a message to be sent.

14. The method according to claim 12 or 13, wherein the MAC value is computed as per RFC2104.

15. The method according to any of the claims 12-14, wherein the method utilizes SHA-1 as the hashing function.

16. The method according to any of the previous claims, wherein the protocol is the SyncML-DM protocol or the SyncML-DS protocol.

17. The method according to any of the previous claims, wherein the protocol is the Obex, http, or WSP protocol.

18. An electronic communication apparatus (1) adapted to provide authentication when messages are exchanged with a server according to a synchronization protocol, **characterized in that** the apparatus is further adapted to incorporate an authentication method indicator (AMI) in an authentication protocol of the synchronization protocol for

indicating a specific type of authentication method, which is determined based on at least one authentication capability of the apparatus (1), according to which the authentication is to be executed.

19. The apparatus according to claim 18, wherein the apparatus (1) is further adapted to send an initialization message to the server for establishing a connection, which message indicates authentication capabilities of the apparatus.

20. The apparatus according to claim 19, wherein the initialization message comprises an authentication method list having at least one authentication method listed, type of apparatus, and/or identity of the apparatus (1).

21. The apparatus according to claim 18, wherein the apparatus (1) is further adapted to determine a type of authentication method to use from the authentication method indicator of a message received from the server (31, 41, 51, 61).

22. The apparatus according to any of the claims 18-21, wherein the apparatus (1) is further adapted to execute any of the steps according to the specified type of authentication method.

23. The apparatus according to claim 22, wherein the apparatus (1) is further adapted to incorporate any authentication data in a data string of a message to be sent according to the synchronization protocol.

24. The apparatus according to any of the claims 18-23, wherein the apparatus (1) is further adapted to provide integrity protection by utilizing an IK (integrity key) for

generating a MAC, and utilizing a hashing function for computing a HMAC on a message to be sent.

25. The apparatus according to claim 24, wherein the apparatus (1) is adapted to compute the MAC value as per RFC2104.

26. The apparatus according to claim 24 or 25, wherein the apparatus (1) is further adapted to utilize SHA-1 as the hashing function.

27. The apparatus according to any of the claims 18-26, wherein the protocol is the SyncML-DM protocol or the SyncML-DS protocol.

28. The apparatus according to any of the claims 18-26, wherein the protocol is the Obex, http, or WSP protocol.

29. The apparatus according to any of the claims 18-28, wherein the apparatus (1) is further adapted to utilize GSM SIM authentication as the authentication method.

30. The apparatus according to any of the claims 18-28, wherein the apparatus (1) is adapted to utilize UMTS USIM authentication as the authentication method and provide server authentication.

31. The apparatus according to any of the claims 18-28, wherein apparatus (1) is further adapted to utilize SecureId, SafeWord, WPKI or WIM authentication as the authentication method.

ART 34 AMDT

32. The apparatus according to any of the claims 18-31, wherein the apparatus is a pager, an electronic organizer, or a smartphone.

33. The apparatus according to any of the claims 18-31, wherein the apparatus is a mobile telephone (1).

34. A server adapted to provide authentication when messages are exchanged with an apparatus (1) according to a synchronization protocol, **characterized in that** the server (31, 41, 51, 61) is further adapted to incorporate an authentication method indicator (AMI) in an authentication protocol of the synchronization protocol for indicating an authentication method, which is determined based on an authentication capability of the apparatus (1), according to which the authentication is to be executed.

35. The server according to claim 34, wherein the server (31, 41, 51, 61) is further adapted to incorporate any authentication data in a data string of the synchronization protocol.

36. The server according to claim 34 or 35, wherein the server (31, 41, 51, 61) is further adapted to determine from a received initialization message authentication capabilities of the apparatus (1) and further determine a specific authentication method to utilize therefrom.

37. The server according to claim 36, wherein the server (31, 41, 51, 61) is further adapted to execute authentication according to the determined authentication method.

38. The server according to any of the claims 34-37, wherein the server (31, 41, 51, 61) is further adapted to

AMENDED SHEET

provide integrity protection by utilizing an IK (integrity key) for generating a MAC, and utilizing a hashing function for computing a HMAC.

39. The server according to claim 38, wherein the server (31, 41, 51, 61) is adapted to derive the MAC value as per RFC2104.

40. The server according to claim 38 or 39, wherein the server (31, 41, 51, 61) is further adapted to utilize SHA-1 as the hashing function.

41. The server according to any of the claims 34-40, wherein the protocol is the SyncML-DM protocol or the SyncML-DS protocol.

42. The server according to any of the claims 34-41, wherein the protocol is the Obex, http, or WSP protocol.

43. The server according to any of the claims 34-42, wherein the server (31, 41, 51, 61) is further adapted to utilize GSM SIM authentication as the authentication method.

44. The server according to any of the claims 34-42, wherein the server (31, 41, 51, 61) is further adapted to utilize UMTS USIM authentication as the authentication method and provide server authentication variable to an electronic user equipment (1).

45. The server according to any of the claims 34-42, wherein server is further adapted to utilize SecureId, SafeWord, WPKI or WIM authentication as the authentication method.